UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

KELLY VRIEZEN, *on behalf of herself and all others similarly situated*, Plaintiff, v. GROUP HEALTH PLAN, INC. d/b/a HEALTHPARTNERS, Defendant.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Kelly Vriezen is a current patient of Group Health Plan, Inc. d/b/a HealthPartners (Group Health Plan or Defendant), who brings this class action against Defendant in her individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions, her counsels' investigation, and upon information and belief as to all other matters, as follows:

1. Plaintiff brings this case to address Defendant's illegal and widespread practice of disclosing Plaintiff's and Class Members' confidential personally identifiable information (PII) and protected health information (PHI) (collectively referred to as Private Information) to third parties, including Meta Platforms, Inc. d/b/a Meta (Facebook).

2. Defendant owns and controls two websites, www.healthpartners.com and www.virtuwell.com (collectively Defendant's Websites or Website), which it encourages

patients to use for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, signing up for events and classes, and more.

3. Defendant installed and implemented the Facebook Tracking Pixel (the Pixel or Facebook Pixel) on its Website, which secretly enables the unauthorized transmission and disclosure of Plaintiff and Class Members' PII and PHI as they are communicated to Defendant.

4. Based on Defendant's use of the Pixel, and evidence demonstrating that the information transmitted via the Pixel was indeed linked to Plaintiff's personal Facebook account, Plaintiff asserts Defendant also installed and implemented the Facebook Conversion Application Programming Interface (Conversion API) on its Website.

5. By implementing Conversions API, Defendant secretly enabled additional unauthorized transmissions and disclosures of Plaintiff and Class Members' PII and PHI.[1]

6. More specifically, Defendant's Websites direct Plaintiff's and Class Members' communications to automatically and surreptitiously be sent to Facebook's servers, and this occurs on every webpage that Defendant has installed the Pixel and Conversions API. [2]

---

[1] "Conversions API works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited: Jan. 25, 2023).

[2] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or

7. Thus, operating as designed and as implemented by Defendant, the Pixel allows the Private Information that Plaintiff and Class Members submit to Defendant to be unlawfully disclosed to Facebook alongside the individual's unique and persistent Facebook ID (FID).

8. Similarly, Conversions API stores Plaintiff's and Class Members' Private Information from visiting Defendant's Website and transmits it to Facebook.

Tracking Pixel

9. A pixel is a piece of code that "tracks the people and the types of actions they take"[3] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), and more.

10. The User's web browser executes the Pixel via instructions within the Defendant's webpage to communicate directly to Facebook certain parameters defined by the Defendant.

11. The Pixel can share the user's Facebook User ID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the

---

optimization in a similar way as other connection channels.", https://developers.facebook.com/docs/marketing-api/conversions-api (last visited: January 27, 2023).

[3] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Jan. 31, 2023).

same web browser. [4] Cookies are only transmitted to the owner site from the user's web browser and cannot be accessed by any other site.

12. The Facebook Pixel is programmable, meaning that the Defendant controls which of its webpages contain the Pixel and which events are tracked and transmitted to Facebook.

13. Pixels are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Upon information and belief, Defendant utilized the Pixel data for marketing purposes in an effort to bolster its profits. Facebook also uses Plaintiff's and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

Conversions API

14. The Facebook Conversions API allows businesses and companies to send web events from their servers to Facebook. [5]

15. The Conversions API is designed to create a direct and reliable connection between marketing data (such as website events and offline conversions) from Defendant's

[4] "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited: January 27, 2023)

[5] https://revealbot.com/blog/facebook-conversions-api/ (last visited: January 24, 2023).

server to Facebook.[6] In doing so, Defendant stores Plaintiff's and Class Members' Private Information on its own server and then transmits it to Facebook from Defendant's server.

16. The Conversions API is an alternative method of tracking versus the Pixel because no privacy protections on the user's end can defeat it. This is because it is Server-Side implementation versus execution by Users' web browsers.

17. Because Conversions API is Server-Side, so it cannot access the Facebook Cookie to retrieve the Facebook User ID.[7] Therefore, other round-about methods of linking the user to their Facebook account must be employed.[8]

18. Facebook has an entire page within its developers' website about how to de-duplicate data received when both a Pixel is executed as well as the Conversions API.[9]

19. Conversions API tracks the user's website interaction, including Private Information, and then transmits this data to Facebook. Indeed, Facebook markets

---

[6] https://www.facebook.com/business/help/204114870265296?id=818859032317965 (last visited: January 25, 2023).

[7] "Our systems are designed to not accept customer information that is unhashed Contact Information, unless noted below. Contact Information is information that personally identifies individuals, such as names, email addresses, and phone numbers, that we use for matching purposes only." https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/ (last visited: January 27, 2023)

[8] "Sending additional customer information parameters may help increase Event Match Quality. Only matched events can be used for ads attribution and ad delivery optimization, and the higher the matching quality, the better." https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req-rec-params (last visited: January 27, 2023)

[9] https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel-and-server-events (last visited: January 27, 2023)

Conversions API as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."

Purpose of this Lawsuit

20. Accordingly, this case arises from Defendant's intentional, reckless, and/or negligent disclosure of Plaintiff's and Class Members' confidential and private medical information to Facebook.

21. The information that Defendant's Pixel and Conversions API sent to Facebook included the Private Information that Plaintiff and Class Members submitted to Defendant's Website, including for example, the type of medical treatment sought, the particular health condition, and the fact that the individual attempted to or did book a medical appointment. Such Private Information would allow a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. This type of disclosure could also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, dementia, or HIV.

22. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers who geotarget Plaintiff's and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and Conversions API.

23. For instance, Plaintiff submitted medical information to Defendant's Website and used the Website to search for a physician, communicate Private Information with her physician, complete patient web forms, and review medical healthcare records.

24. Shortly thereafter, this information was communicated from Defendant's Website to Facebook.

25. Defendant regularly encourages Plaintiff and Class Members to use its digital tools, including its Website, to receive healthcare services. Plaintiff and Class Members provided their Private Information through Defendant's Website with the reasonable understanding that Defendant would secure and maintain any PII and PHI as confidential.

26. At all times that Plaintiff and Class Members visited and utilized Defendant's Website, they had a reasonable expectation of privacy in the Private Information collected through Defendant's Website, including that it would remain secure and protected and only utilized for medical purposes.

27. Plaintiff and Class Members provided Private Information to Defendant in order to receive medical services rendered and with the reasonable expectation that Defendant would protect their Private Information. Plaintiff and Class Members relied on Defendant to secure and protect the Private Information and not disclose it to unauthorized third parties without their knowledge or consent.

28. Defendant further made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchange with Defendant.

29. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiff's and Class Members' Private Information safe, secure, and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

30. Defendant, however, failed in its obligations and promises by utilizing the Facebook Pixel and Conversions API, described below, on its Website, knowing that such technology would transmit and share Plaintiff's and Class Members' Private Information with Facebook.

31. While Defendant willfully and intentionally incorporated the Pixel and Conversions API into its Website, Defendant has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications via the Website with Facebook. As a result, Plaintiff and Class Members were unaware that their PII and PHI were being surreptitiously transmitted to Facebook as they communicated with their healthcare provider via the Website.

32. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web based technology to ensure the Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the consent of Plaintiff and Class Members to disclose their PII and PHI to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' PII and PHI

through Facebook Pixels; (v) failing to warn Plaintiff and Class Members; and (vi) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient PII and PHI.

33. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Pixel, (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information, (v) statutory damages, and (v) the continued and ongoing risk to their Private Information.

34. Plaintiff seeks to remedy these harms and bring causes of action for (1) Invasion of Privacy, (2) unjust enrichment; (3) breach of implied contract; (4) violations of the Electronics Communication Privacy Act (ECPA) 18 U.S.C. § 2511(1) -unauthorized interception, use, and disclosure; (5) violations of ECPA, 18 U.S.C. § 2511(3)(a) - unauthorized interception, use, and disclosure; (6) violations of Title II of the ECPA, 18 U.S.C. § 2702, *et seq*., - Stored Communications Act; (7) violations of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, *et seq*.; and (8) breach of confidence.

PARTIES

Plaintiff Kelly Vriezen

35. Plaintiff is a natural person and citizen of Minnesota where she intends to remain. On numerous occasions, Plaintiff accessed Defendant's Website on her mobile device and/or computer. Plaintiff used the Website to find and obtain medical treatment. Pursuant to the systematic process described in this Complaint, Plaintiff's Private

Information was disclosed to Facebook, and this data included her PII, PHI, and related confidential information. Defendant intercepted and/or assisted these interceptions without Plaintiff's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff's PII and PHI.

36. Plaintiff Vriezen has received healthcare services since 2017 at one of the hospitals in Defendant's network and has used Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

37. Plaintiff Vriezen has been using Defendant's Website, including the Virtuwell Webpage since 2017.

38. Plaintiff Vriezen used Defendant's Website, including the Virtuwell Webpage, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

39. Plaintiff Vriezen has been a Facebook user since 2009.

40. Plaintiff Vriezen accessed Defendant's Website, including the Virtuwell Webpage, to receive healthcare services from Defendant or Defendant's affiliates, at Defendant's direction, and with Defendant's encouragement.

41. As Defendant's patient, Plaintiff Vriezen reasonably expected that her online communications with Defendant were solely between herself and Defendant and that such communications would not be transmitted or intercepted by a third party. Plaintiff also

relied on Defendant's Privacy Policies in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff would not have disclosed her Private Information to Defendant.

42. During her time as a patient, Plaintiff Vriezen never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information.

43. Notwithstanding, through the Pixel and Conversions API, Defendant transmitted Plaintiff Vriezen's Private Information to third parties, such as Facebook and Google.

Defendant Group Health, Inc. d/b/a Healthpartners

44. Defendant Group Health, Inc. d/b/a HealthPartners is headquartered at 8170 33rd Ave., S. Bloomington, MN 55425. Defendant is an integrated health care organization providing health care services and health plan financing and administration, and it was founded in 1957 as a cooperative. Defendant is the largest consumer governed nonprofit health care organization in the nation – serving more than 1.8 million medical and dental health plan members nationwide. Its care system includes a multi-specialty group practice of more than 1,800 physicians that serves more than 1.2 million patients. HealthPartners employs over 26,000 people, "all working together to deliver the HealthPartners mission."[10]

[10] https://www.healthpartners.com/about/ (last visited: Jan. 10, 2023).

45. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 (HIPAA))

JURISDICTION & VENUE

46. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendant.

47. This Court has federal question jurisdiction under 29 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (28 U.S.C. § 2511, *et seq.*, and 28 U.S.C. § 2702) and the CFAA (18 U.S.C. § 1030, *et seq*).

48. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

49. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

A. Background: Underlying Technology Employed by Defendant for the Purpose of Disclosing Plaintiff and Class Members' Private Information to Facebook.

50. Defendant purposely installed the Pixel and Conversions API tools on many of its webpages within its Website, and it programmed those webpages to surreptitiously

share its patients' private and protected communications with Facebook, including communications that contain Plaintiff's and Class Members' PHI and PII.

51. Defendant uses the Website to connect Plaintiff and Class Members to Defendant's digital healthcare platforms with the goal of increasing profitability.

52. In order to understand Defendant's unlawful data-sharing practices, it is important first to understand basic web design and tracking tools.

i. Facebook's Business Tools and the Pixel.

53. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[11]

54. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

55. Facebook's Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

56. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal

[11] Facebook, *Meta Reports Fourth Quarter and Full Year 2021 Results* , https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022)

Resource Locator ("URL") and metadata, button clicks, etc.[12] Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[13]

57. One such Business Tool is the Pixel that "tracks the people and type of actions they take."[14] When a user accesses a webpage that is hosting the Pixel, the communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers—traveling from the user's browser to Facebook's server.

58. Notably, this transmission only occurs on webpages that contain the Pixel. Thus, Plaintiff's and Class Member's Private Information would not have been disclosed to Facebook via the Pixel but for Defendant's decisions to install the Pixel on its Website.

59. Similarly, Plaintiff's and Class Member's Private Information would not have been disclosed to Facebook via Conversions API but for Defendant's decision to install and implement that tool.

---

[12] Facebook, *Specifications for Facebook Pixel Standard Events,* https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Jan. 31, 2023); *see* Facebook, *Facebook Pixel, Accurate Event Tracking, Advanced*, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Facebook, *Best Practices for Facebook Pixel Setup*, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; Facebook, *App Events API*, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 31, 2023).

[13] Facebook, *About Standard and Custom Website Events*, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* Facebook, *App Events API*, *supra*.

[14] Facebook, *Retargeting*, https://www.facebook.com/business/goals/retargeting.

60. By installing and implementing both tools, Defendant caused Plaintiff's and Class Member's communications to be intercepted and transmitted to Facebook via the Pixel, and it caused a second improper disclosure of that information via Conversions API.

61. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via certain webpages.

ii. Defendant's method of transmitting Plaintiff's and Class Members' Private Information via the Pixel and/or Conversions API i.e., the interplay between HTTP Requests and Responses, Source Code, and the Pixel

62. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as computer, tablet, or smart phone) accessed web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

63. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

64. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET

Requests can also send data to the host server embedded inside the URL, and can include cookies. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF for filing a motion to a court).

- **Cookies**: a small text file that can be used to store information on the client device that can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.[15]

65. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as a physician's "Book an Appointment" page). The HTTP Response sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Website.

66. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain

[15] One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

actions when the web page first loads or when a specified event triggers the code.

67. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When patients visit Defendant's website via an HTTP Request to HealthPartner's or Virtuwell's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel. Thus, Defendant is, in essence, handing patients a tapped phone, and once the Webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook.

68. Third parties, like Facebook, place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the patient associated with the Private Information intercepted.

69. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that savvy users cannot evade. Facebook's workaround, for example, is called Conversions API. Conversions API is an effective workaround because it does the transmission from their

own servers and does not rely on the User's web browsers. Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."[16] Thus, the communications between patients and Defendant, which are necessary to use Defendant's Website, are actually received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

70. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like Conversions API without access to the host server, companies like Facebook instruct Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[17] Thus, it is reasonable to infer that Facebook's customers who implement the Facebook Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround.

71. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user's

[16] Facebook, *Prepare your Business to Use the Conversions API,* https://www.facebook.com/business/help/129506453084120 7?id=818859032317965 (last accessed Jan. 31, 2023).

[17] *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Jan. 23, 2023).

communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner (*i.e.,* to bolster profits).

72. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

73. In this case, Defendant employed the Pixel and Conversions API to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook.

74. For example, when patients visit www.healthpartners.com/care/specialty/ and selects "Neuroscience," the patient's browser automatically sends an HTTP Request to Defendant's web server. Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage as depicted below.

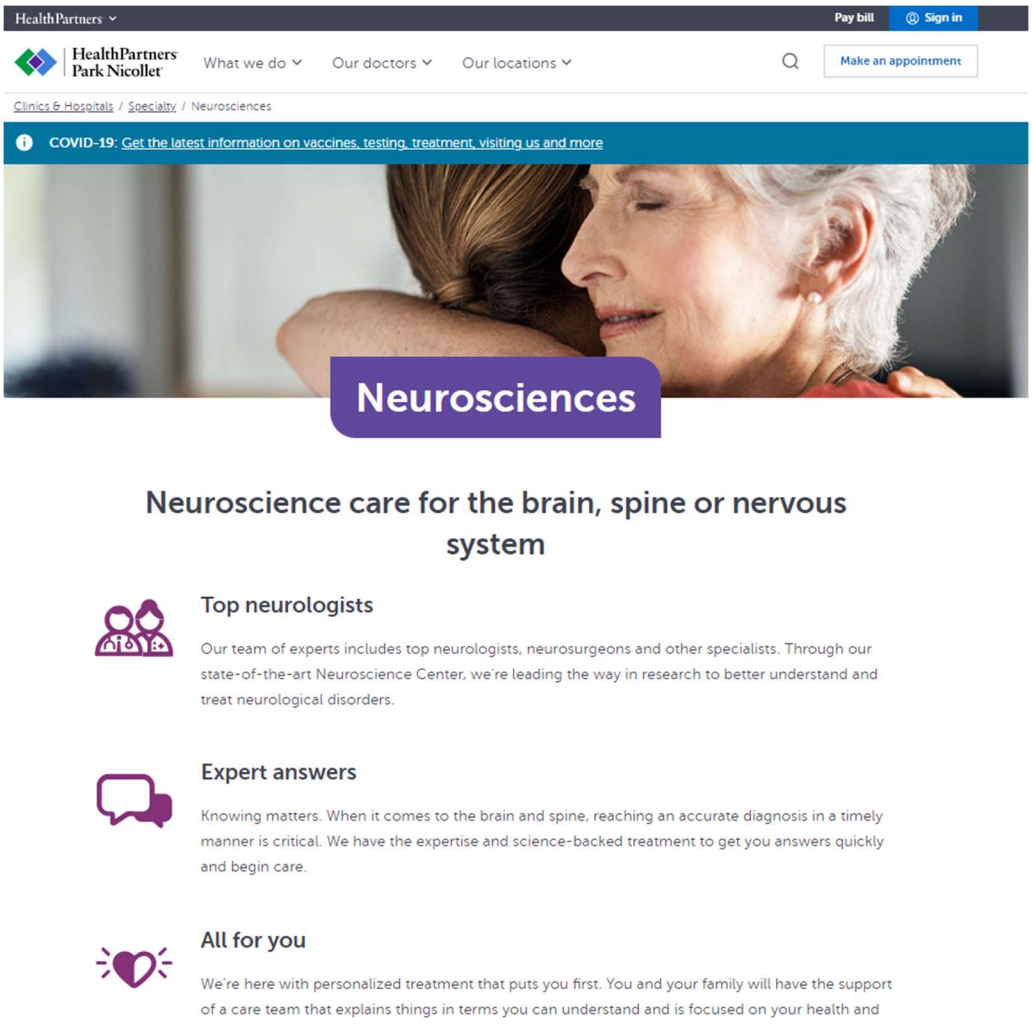


Figure 1 Image taken from https://www.healthpartners.com/care/specialty/neuroscience/.

75. The patient visiting this particular web page only sees the Markup, not the Defendant's Source Code or underlying HTTP Requests and Responses.

76. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions and can command a website visitor's browser to send data transmissions to third parties via pixels or web bugs,[18] effectively open a spying

[18] These pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware

window through which the webpage can funnel the visitor's data, actions, and communications to third parties.

77. Looking to the previous example, Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) and send those communications to Facebook.

78. This occurs because the Pixel embedded in Defendant's Source Code is programmed to automatically track and transmit patient's communications, and this occurs contemporaneously, invisibly, and without the patient's knowledge.

79. Thus, without its patients' consent, Defendant has effectively used its Source Code to commandeer patients' computing devices, thereby re-directing their Private Information to third parties.

80. The information that Defendant's Pixel sends to Facebook may include, amongst other things, patients' PII, PHI, and other confidential information.

81. Consequently, when Plaintiff and Class Members visit Defendant's website and communicate their Private Information, it is transmitted to Facebook, including, but not limited to, appointment type and date, physician selected, specific button/menu selections, content typed into free text boxes, demographic information, email addresses, phone numbers, and emergency contact information.

B. Defendant's Pixel and/or Conversions API Tracking Practices caused Plaintiff's and Class Members' PII and PHI to be sent to Facebook.

---

of them.

82. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel and Conversions API on its Website to secretly track patients by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties and obligations.[19]

83. Defendant's Webpages contain a unique identifier that indicates that the Pixel is being used on a particular webpage, identified as 1113456592041476 on www.heathpartners.com and 200310607002735 on www.virtuwell.com.

84. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs.[20] However, Defendant's Website does not rely on the Pixel in order to function.

85. While seeking and using Defendant's services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendant via its Website.

86. Plaintiff and Class Members were not aware that their Private Information would be shared with Facebook as it was communicated to Defendant because, amongst other things, Defendant did not disclose this fact.

87. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to Facebook, nor did they intend for Facebook to be a party to their communications with Defendant.

88. Defendant's Pixel and Conversions API sent non-public Private Information

[19] *Id.*

[20] *Id.*

to Facebook, including but not limited to Plaintiff's and Class Members': (1) status as medical patients; (2) health conditions; (3) sought treatment or therapies; (4) appointment requests and appointment booking information; (5) registration or enrollment in medical classes (such as breastfeeding courses); (6) locations or facilities where treatment is sought; (7) which webpages were viewed; and (8) phrases and search queries conducted via the general search bar.

89. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside the Plaintiff's and Class Members' Facebook ID (c_user cookie or "FID"), thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts.[21]

90. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

91. Defendant deprived Plaintiff and Class Members of their privacy rights when

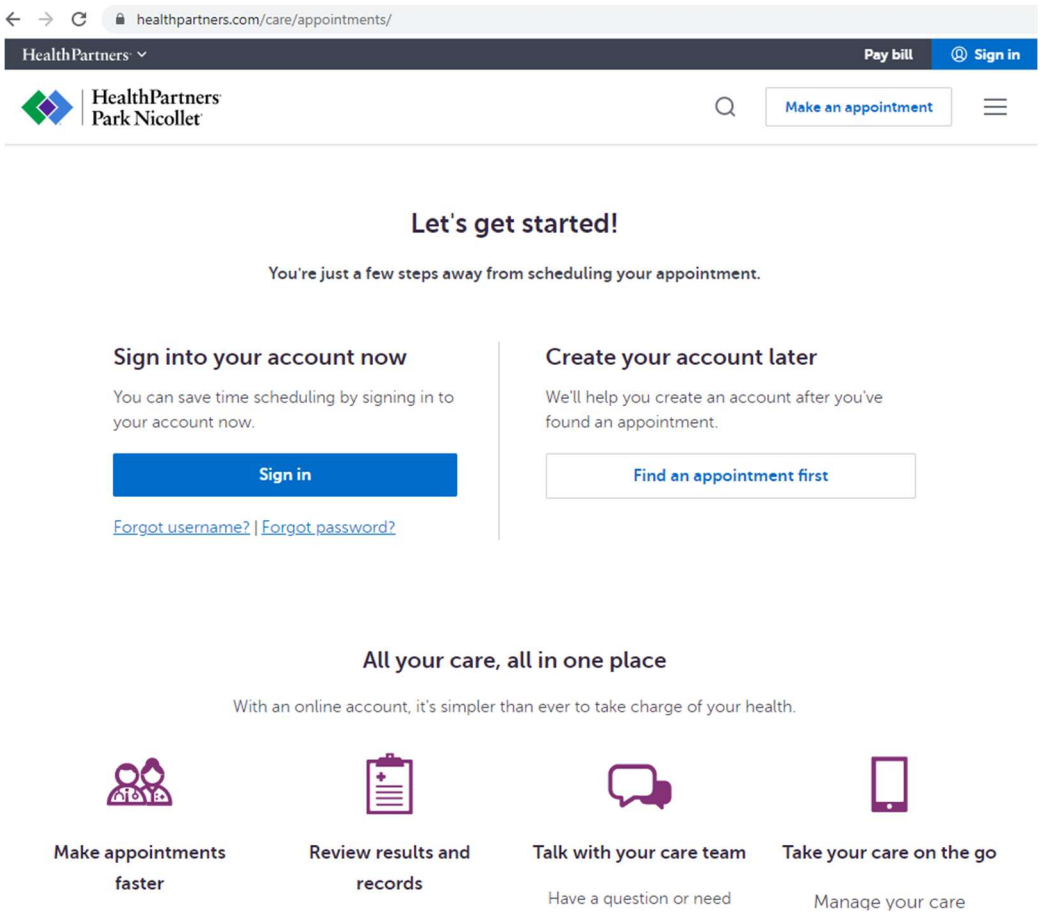
[21] Defendant's Website track and transmit data via first-party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

it: (1) implemented technology (i.e., the Facebook Pixel and Conversions API) that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Facebook—an unauthorized third-party; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

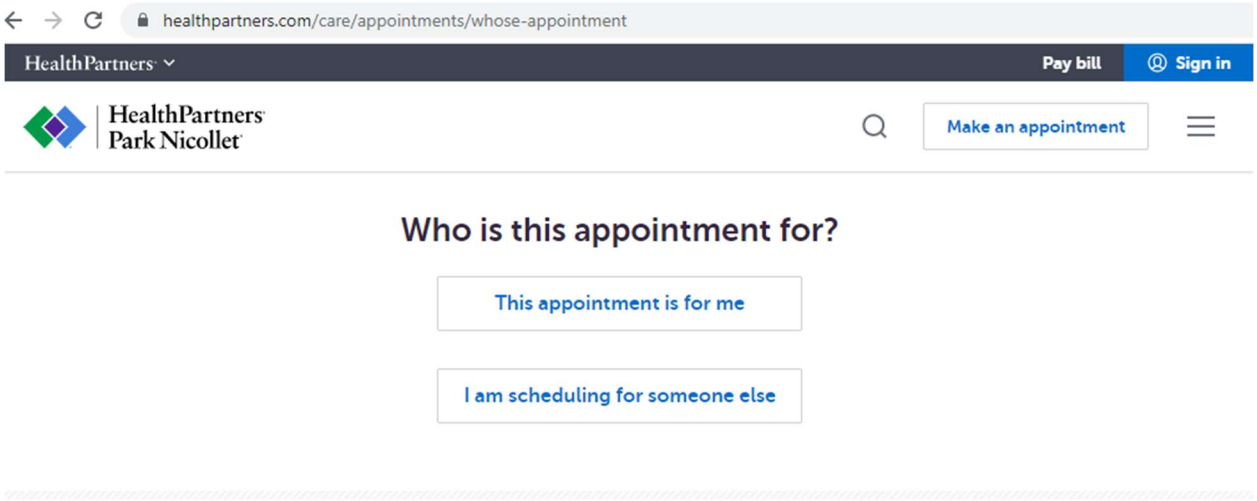
i. Defendant's Pixel Disseminates Patient Information via www.HealthPartners.com.

92. An example illustrates the point. If a patient uses www.healthpartners.com to book an appointment with an gynecologist for the purpose of obtaining birth control, Defendant's Webpage directs them to a series of screens that ask the patient to communicate additional information. Unbeknownst to the patient, each and every communication is sent to Facebook via Defendant's Pixel, as evidenced by the images below.

93. In order to book an appointment, the user visits www.healthpartners.com/care/appointments and clicks the "Find an appointment first" button.

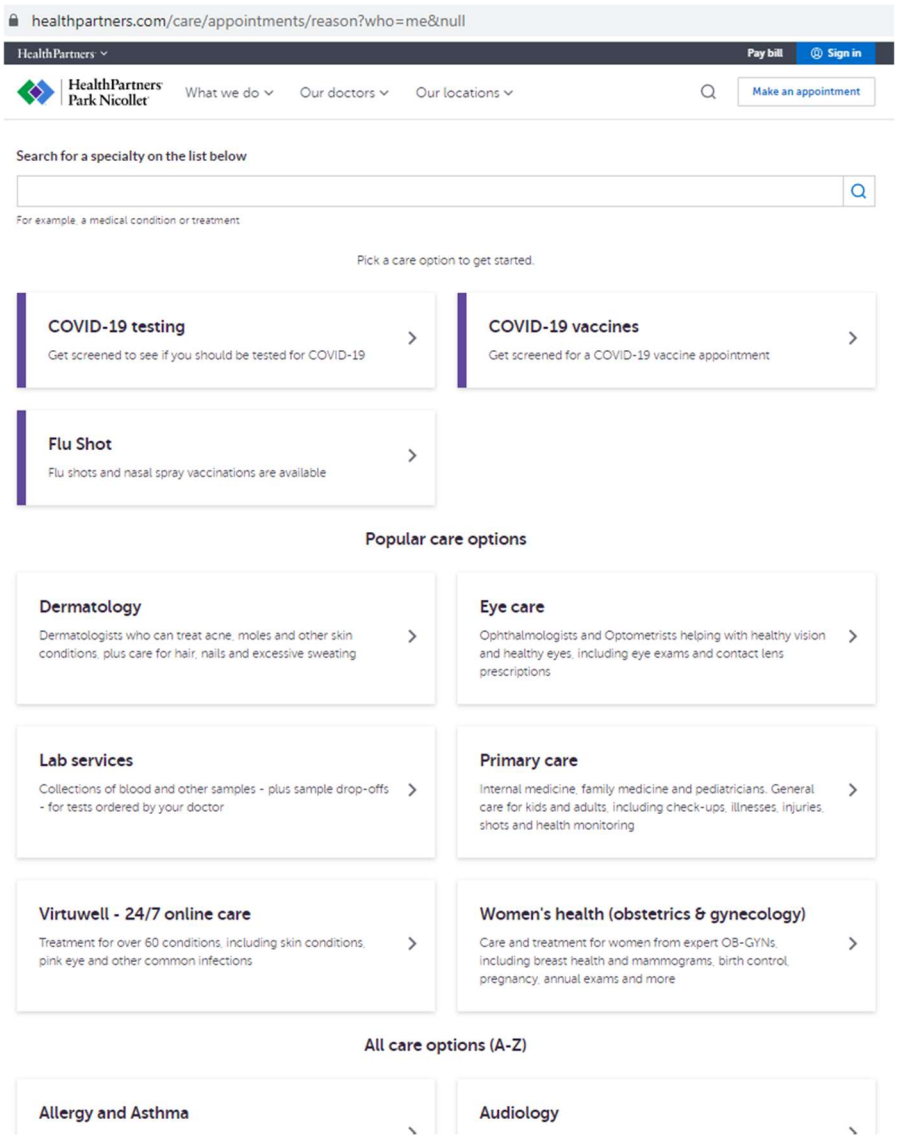


94. Next, the user clicks the "This appointment is for me" button.

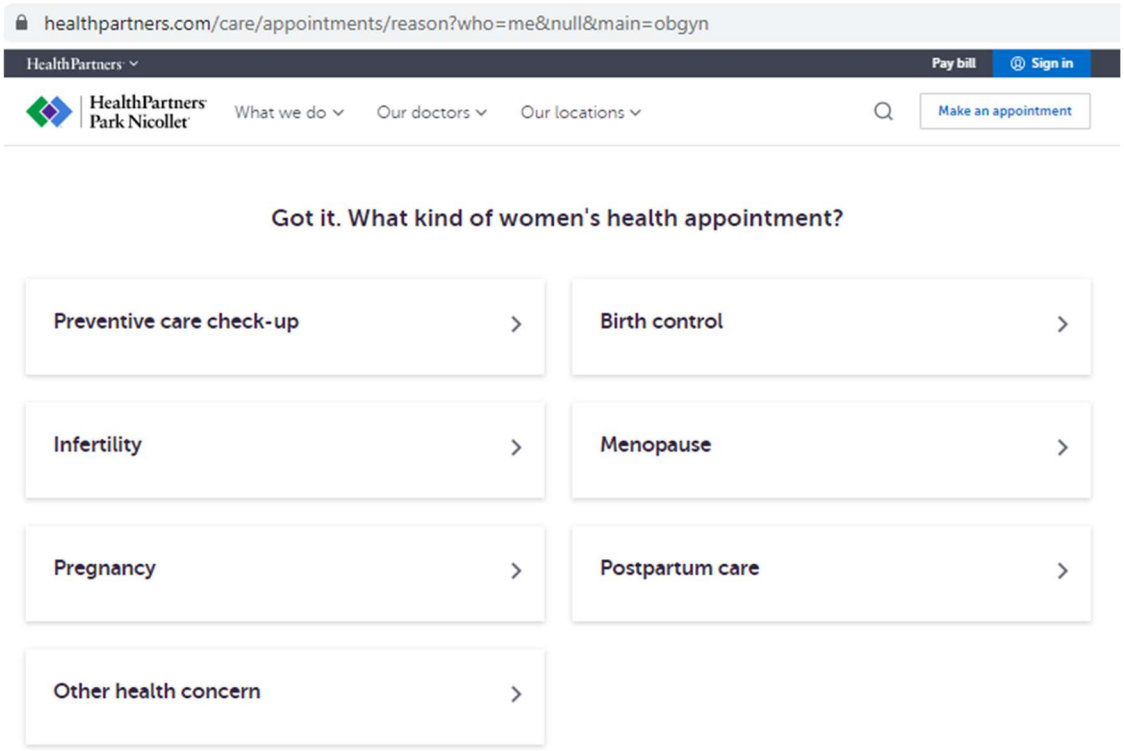


95. Defendant then directs the user to narrow their appointment search results by

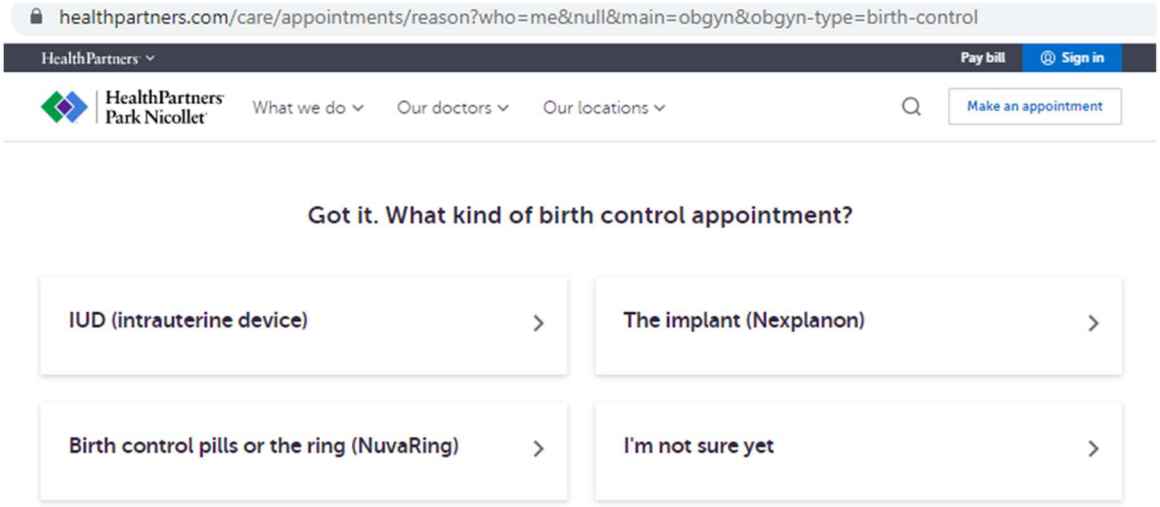
either typing a medical condition or treatment into the search bar or choosing from a list of "popular care options" or "All care options (A-Z)."



96. The user clicks the "Women's health (obstetrics & gynecology)" button, and Defendant directs them to identify the "reason" for the appointment, or what type of appointment the user believes they need, by selecting the course of treatment, symptom, or health condition for which they are seeking treatment.

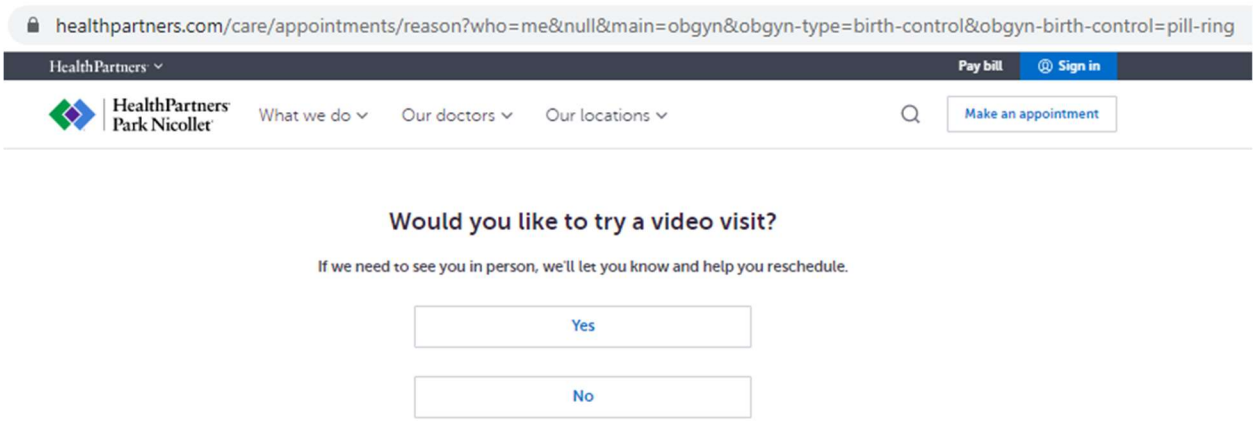


97. Upon clicking the "birth control" button, Defendant asks the user to identify which type of treatment they are seeking.

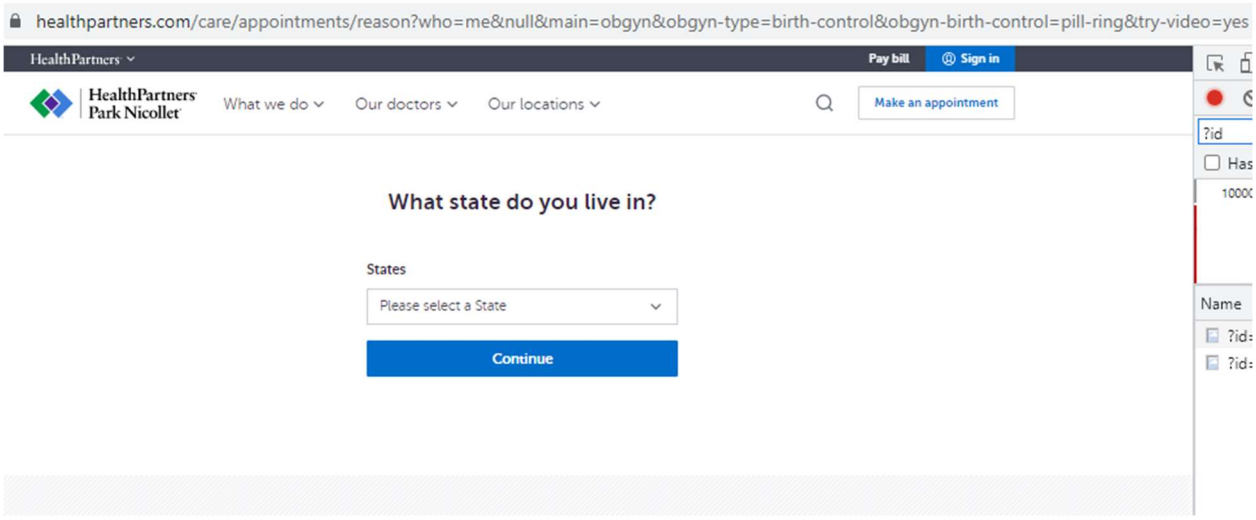


98. Upon clicking the "Birth control pills or the ring (NuvaRing)" button, Defendant asks whether the user would like to schedule a video visit or in-person

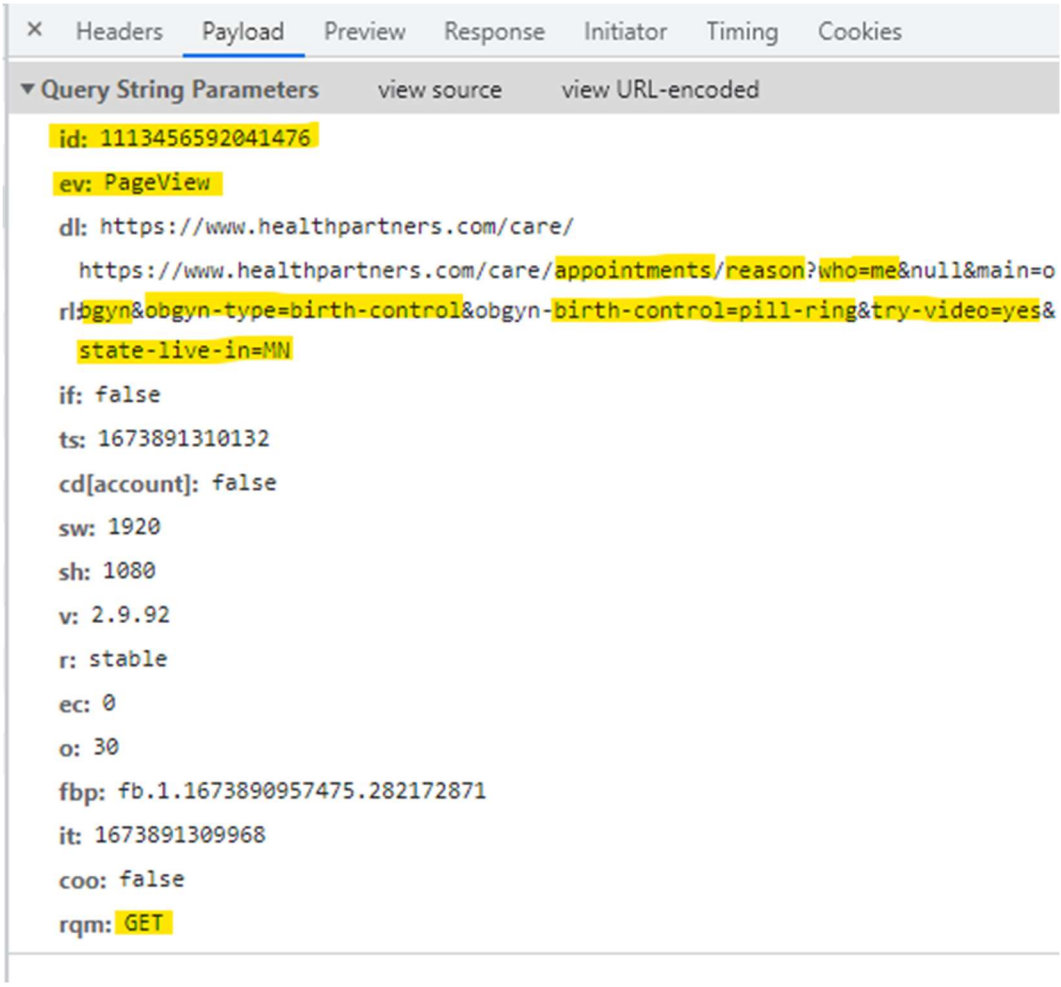
appointment.



99. Upon clicking the "Yes" button, Defendant asks the user to identify their location, and the user selects Minnesota from the drop-down menu below.



100. Without alerting the user, Defendant's Pixel sends each and every communication the user made to the Defendant via the Webpage to Facebook, and the image below confirms that the communications Defendant sends to Facebook contain the user's Private Information.



101. The first line of highlighted text, "id: 1113456592041476," refers to the Defendant's Pixel ID for this particular Webpage and confirms that the Defendant has downloaded the Pixel into its Source Code on this particular Webpage.

102. The second line of text, "ev: PageView," identifies and categorizes which actions the user took on the Webpage ("ev:" is an abbreviation for event, and "PageView" is the type of event). Thus, this identifies the user as having viewed the particular Webpage.

103. The remaining lines of text identify: (1) the user as a patient seeking medical care from Defendant via www.healthpartners.com; (2) who is in the process of booking an

"appointment"; (3) the appointment is for herself as opposed to someone else (appearing as "who=me" in the text above); (4) the appointment is with an "obgyn" (aka the "reason" for the appointment); (5) the medical treatment and sought medication is "birth control"; (6) the user has identified which type of birth control they desire ("pill-ring"); (7) the user's location ("state-live-in=MN" with "MN"(Minnesota); and (8) the fact that the user's appointment will be via video instead of in-person ("try-video=yest").

104. Finally, the last line of highlighted text ("GET"), demonstrates that Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the user's Facebook ID (c_user ID). This is further evidenced by the image below, which was collected during the same browsing session as the previous image.[22]

[22] The user's Facebook ID is represented as the c_user ID highlight in the image above, and Plaintiff has redacted the corresponding string of numbers to preserve the user's anonymity.

▼ Request Headers

:authority: www.facebook.com
:method: GET
:path: /tr/?id=1113456592041476&ev=PageView&dl=https%3A%2F%2Fwww.healthpartners.com%2Fcare%2F&rl=https%3A%2F%2Fwww.healthpartners.com%2Fcare%2Fappointments%2Freason%3Fwho%3Dme%26null%26main%3Dobgyn%26obgyn-type%3Dbirth-control%26obgyn-birth-control%3Dpill-ring%26try-video%3Dyes%26state-live-in%3DMN&if=false&ts=1673891310132&cd[account]=false&sw=1920&sh=1080&v=2.9.92&r=stable&ec=0&o=30&fbp=fb.1.1673890957475.282172871&it=1673891309968&coo=false&rqm=GET
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
cookie: sb=VrLBY5y36a3RDUuvDZHMHwFK; datr=VrLBYwe38VyhLPXyBwHdGCHz; locale=en_GB; c_user=[redacted] xs=16%3Adc-OmvjWvJCxQw%3A2%3A1673890850%3A-1%3A2663; fr=0Lk2J0HBqeRNMmtFP.AWUfKZOJnzvJbABUps7sZ2Bg0CA.BjwfzB.IK.AAA.0.0.BjxYwj.AWUcjnkPLRU
referer: https://www.healthpartners.com/
sec-ch-ua: "Not_A Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
sec-fetch-dest: image
sec-fetch-mode: no-cors
sec-fetch-site: cross-site
user-agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36

105. In addition to tracking its patients' "PageViews," Defendant's Pixel is also tracking and transmitting information about which buttons a user clicks or selects during their browsing session. In the example below, the user's Webpage activity is categorized and communicated to Facebook as a "SubscribedButtonClick," indicating which buttons the user selected on the Webpage.

▼ Request Headers

:authority: www.facebook.com

:method: GET

:path: /tr/?id=1113456592041476&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.healthpartners.com%2Fcare%2Fspecialty%2Fwomens-health%2Fob-gyn%2F&rl=https%3A%2F%2Fwww.healthpartners.com%2Fcare%2Fspecialty%2F&if=false&ts=1674068655640&cd[buttonFeatures]=%7B%22classList%22%3A%22hp-call-to-action%20md%20primary%22%2C%22destination%22%3A%22https%3A%2F%2Fwww.healthpartners.com%2Fcare%2Fappointments%2Fstart%3Fmain%3Dobgyn%22%2C%22id%22%3A%220100007900800227-primary1%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Schedule%20online%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22%3A%22%22%7D&cd[buttonText]=Schedule%20online&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22OB-GYN%20(Obstetrics%20%26%20Gynecology)%20%7C%20HealthPartners%20%26%20Park%20Nicollet%20%22%7D&sw=1920&sh=1080&v=2.9.92&r=stable&ec=2&o=30&cs_est=true&fbp=fb.1.1673890957475.282172871&it=1674068635272&coo=false&es=automatic&tm=3&rqm=GET

:scheme: https

accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

accept-encoding: gzip, deflate, br

accept-language: en-US,en;q=0.9

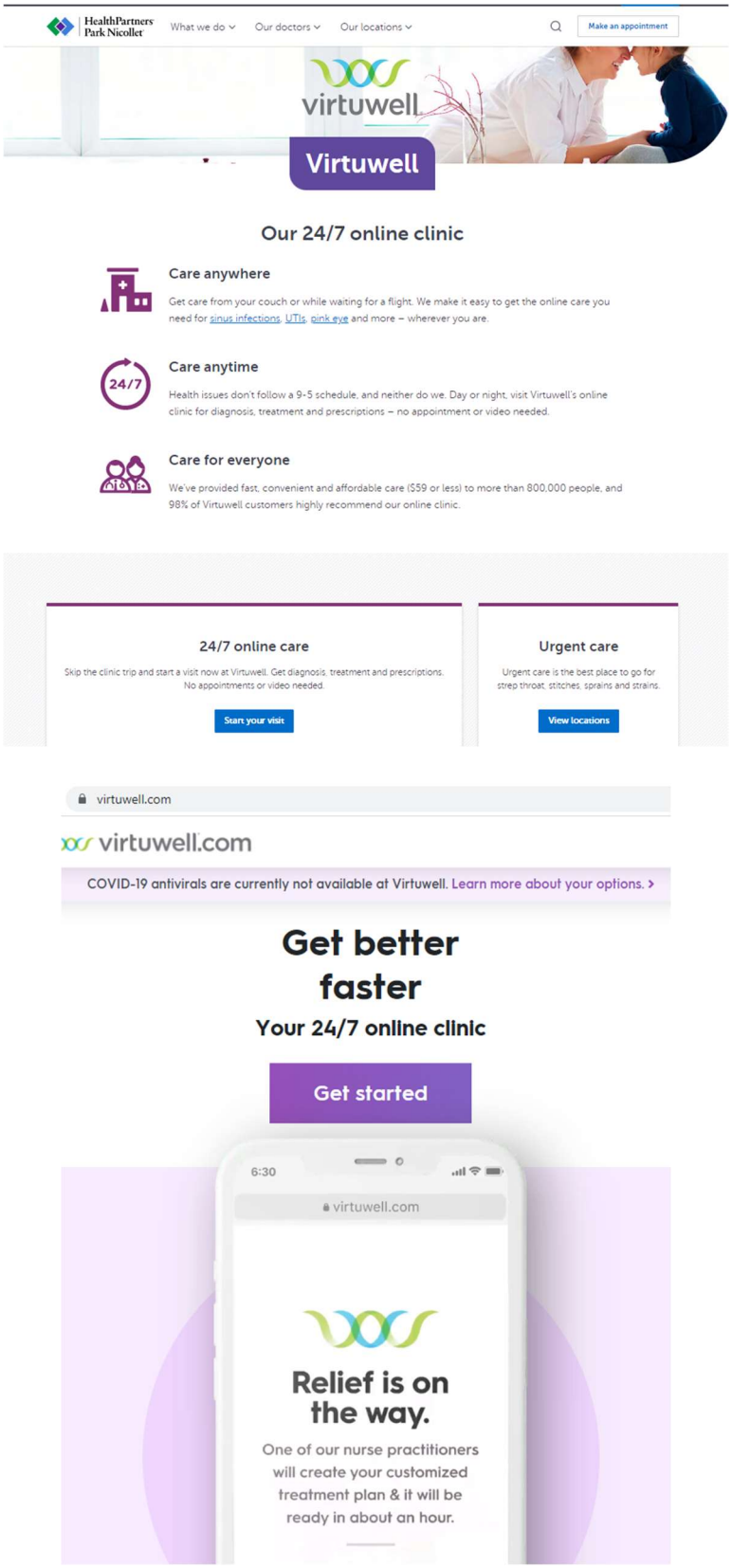
cookie: sb=VrLBY5y36a3RDUuvDZHMHwFK; datr=VrLBYwe38VyhLPXyBwHdGCHz; locale=en_GB; c_user=[redacted] xs=16%3Adc-OmvjWvJCxQw%3A2%3A1673890850%3A-1%3A2663%3A%3AAcWVoxULZBiUrHj90nvqoQ_Dh_XkVzoPghqlFAWG7w; fr=0PuPbpkHkSB9mv3gD.AWWuM0oW1acqBnIvCNx03ORTG9Y.BjyC8r.IK.AAA.0.0.BjyC8r.AWWnMQRpe5Q

referer: https://www.healthpartners.com/

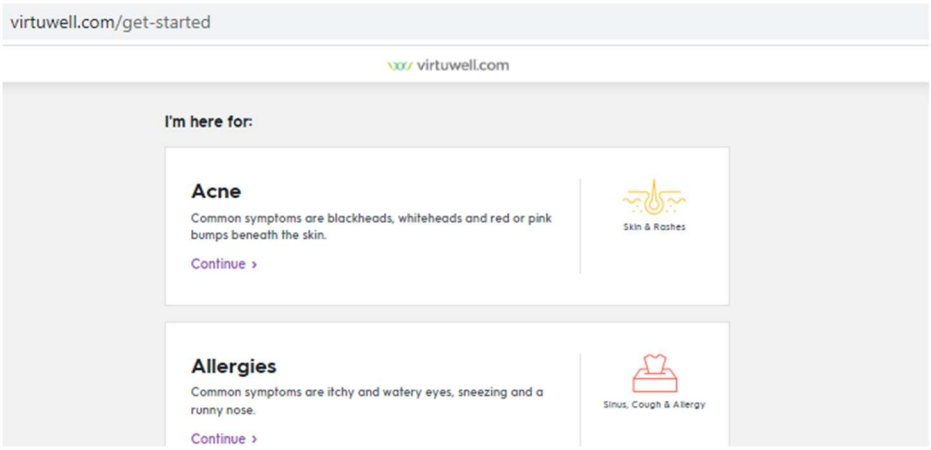
sec-ch-ua: "Not_A Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"

ii. Defendant's Pixel Disseminates Patient Information via Virtuwell.com and other Websites

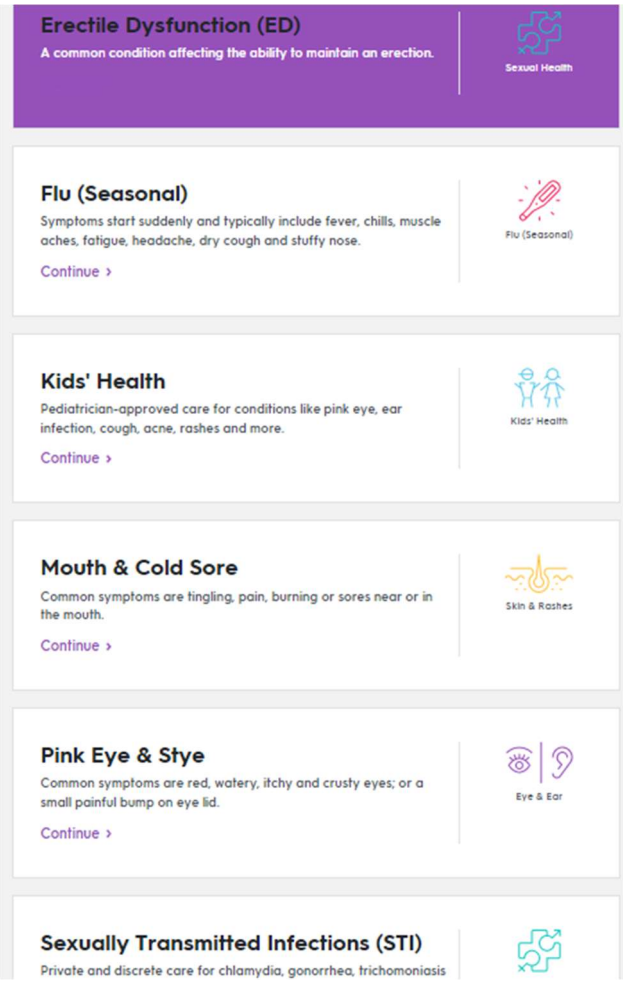
106. Defendant encourages its patients to use "Virtuwell," which it describes as a "24/7 online clinic." Upon clicking the "Start your visit" button in the image below, Defendant directs the user to virtuwell.com where the user must click the "Get started" button to continue.


HealthPartners Park Nicollet
What we do
Our doctors
Our locations
Make an appointment
virtuwell
Virtuwell
Our 24/7 online clinic
Care anywhere
Get care from your couch or while waiting for a flight. We make it easy to get the online care you need for sinus infections, UTIs, pink eye and more – wherever you are.
Care anytime
24/7
Health issues don't follow a 9-5 schedule, and neither do we. Day or night, visit Virtuwell's online clinic for diagnosis, treatment and prescriptions – no appointment or video needed.
Care for everyone
We've provided fast, convenient and affordable care ($59 or less) to more than 800,000 people, and 98% of Virtuwell customers highly recommend our online clinic.
24/7 online care
Skip the clinic trip and start a visit now at Virtuwell. Get diagnosis, treatment and prescriptions. No appointments or video needed.
Start your visit
Urgent care
Urgent care is the best place to go for strep throat, stitches, sprains and strains.
View locations
virtuwell.com
virtuwell.com
COVID-19 antivirals are currently not available at Virtuwell. Learn more about your options. ›
Get better faster
Your 24/7 online clinic
Get started
6:30
virtuwell.com
Relief is on the way.
One of our nurse practitioners will create your customized treatment plan & it will be ready in about an hour.

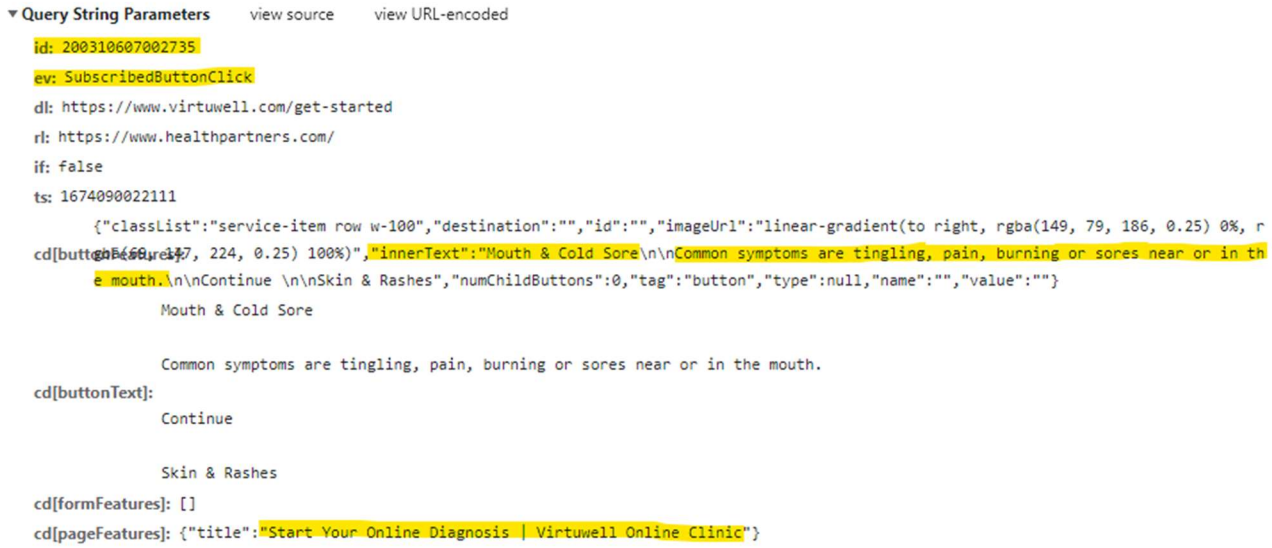
107. Next, Defendant asks the user to identify what type of treatment they are seeking by selecting the health condition or symptom they are experiencing.



108. The user selects "Mouth & Cold Sore" and clicks the "Continue" button.

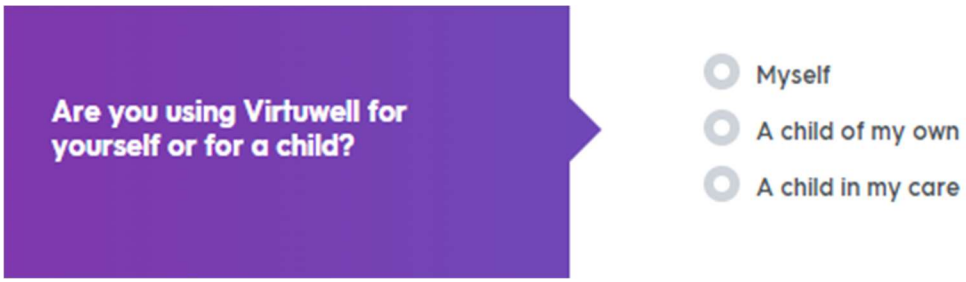


109. Upon doing so, Defendant's Pixel records the user's activity as a "SubscribedButtonClick" event and sends that information to Facebook. The image below demonstrates that Defendant's Pixel is located on this particular Webpage (recorded as id: 200310607002735 for this particular Webpage and highlighted in the image below).

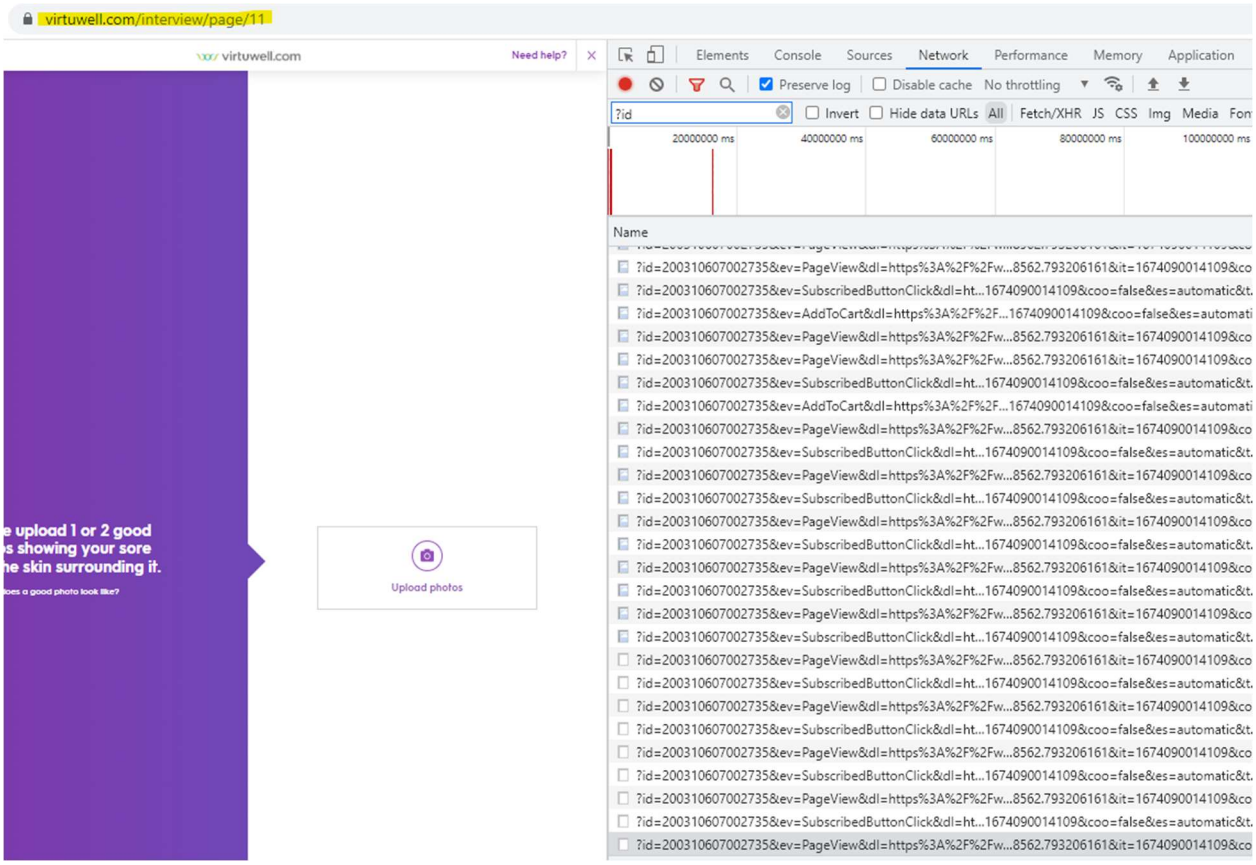


110. Next, the user clicks "Start Interview." Upon doing so, Defendant's Pixel records and transmits the user's activity to Facebook, categorizing it as a "SubscribedButtonClick" event, "AddToCart" event, and "PageView." As with previous examples, Defendant's Pixel sends this information alongside the user's unique and persistent Facebook ID.

111. Next, Defendant asks the user to specify who the appointment is for.



112. Upon selecting "Myself" and clicking "Continue," Defendant's Pixel once again sends the user's communication to Facebook. As the user continues through the interview process, Defendant asks the user to communicate additional PHI and PII on each new Webpage. By the eleventh Webpage, Defendant's Pixel has sent the user's communications to Facebook approximately 25 times. The image below is a screenshot taken from virtuwell.com/interview/page/11, and the column to the right lists each instance in which the user's communications with Defendant were transmitted to Facebook via the Defendant's Pixel.



113. Defendant's practice of transmitting its patients' data extends beyond its own website. For example, Defendant offers and encourages its patients to sign up for healthcare classes, events, and support groups including breastfeeding courses, a "Community Foot Care Clinic," "Better Breathers" courses, and "Stomp out diabetes" online courses. If a patient attempts to book an online breastfeeding course, Defendant's Webpage redirects the patient to a third-party website to complete their booking (https://www.eventbrite.com/e/breastfeeding-online-stillwater-registration-444739205937).

114. From there, the patient can select a desired date, submit additional information, and purchase the event ticket.

115. As with the other examples, the patient's information is communicated to Facebook via the Defendant's Pixel, and Defendant has purposefully designed its events to track patient's activity and communications.

116. The tracking that occurs is not the result of a pre-programmed function, but rather a purposeful decision made by Defendant. As the instructions below explain, Eventbrite allows the event host (Defendant) to configure and program a particular event's webpage.[23] In conjunction with this, the event host can upload their tracking pixel.

[23] https://www.eventbrite.com/support/articles/en_US/Multi_Group_How_To/how-to-create-a-tracking-pixel-with-facebook?lg=en_US (last accessed Jan. 18, 2023).

Add your pixel to your Eventbrite event

1. Go to your event dashboard.

Go to **Manage events** in your account. Then select your event.

2. Go to "Tracking pixels" (under "Marketing").

3. Click "Facebook pixel" and enter your Facebook pixel ID.

Choose between "This event" and "All events".

- **This event** — This pixel will only be on your current event. It won't be included if the event is copied.
- **All events** — This pixel is on all events on your account, even ones you create later.

4. Optional: Create additional events.

By default, your Facebook pixel fires the following standard actions:

- **Pageview** when people load your event listing
- **Purchase** when they complete their order

If you need to collect more information:

1. Click **Add standard event**.
2. Choose when you want this event to fire.
3. Select the label for this event.

You have the following options for when to fire:

- **Event listing** — when attendees visit your event page
- **Event register** —when attendees view the order form
- **Event order confirmation** — when attendees complete a purchase
- **Reserved seating pick a seat** — when attendees choose a seat for a reserved seating event

The **website action** affects how your pixel appears in your data. For example, if you want your pixel to fire when someone gets to the order form, you might choose **Event register** and **Website checkouts initiated**.

5. Save your changes.

117. Correspondingly, on information and belief, the images below demonstrate that Defendant has indeed implemented its Pixel to track and transmit information to Facebook whenever patients book healthcare related courses.

▼ Query String Parameters view source view URL-encoded

id: 1595986097313505

ev: PageView

dl: https://www.eventbrite.com/e/breastfeeding-class-tickets-458670404527

rl: https://www.healthpartners.com/

if: false

ts: 1674096687006

sw: 1920

sh: 1080

v: 2.9.92

r: stable

ec: 0

o: 30

fbp: fb.1.1673907027801.1413207497

it: 1674096686773

coo: false

exp: b3

rqm: GET

▼ Query String Parameters view source view URL-encoded

id: 1595986097313505

ev: SubscribedButtonClick

dl: https://www.eventbrite.com/checkout-external?eid=458670404527&parent=https%3A%2F%2Fwww.eventbrite.com%2Fe%2Fbreastfeeding-class-tickets-458670404527&modal=1&aff=oddtdteb

rl: https://www.eventbrite.com/e/breastfeeding-class-tickets-458670404527

if: true

ts: 1674098338655

cd[buttonFeatures]: {"classList":"eds-btn eds-btn--button eds-btn--fill","destination":"","id":"","imageUrl":"","innerText":"Tickets","numChildButtons":0,"tag":"button","type":"button","name":"","value":""}

cd[buttonText]: Tickets

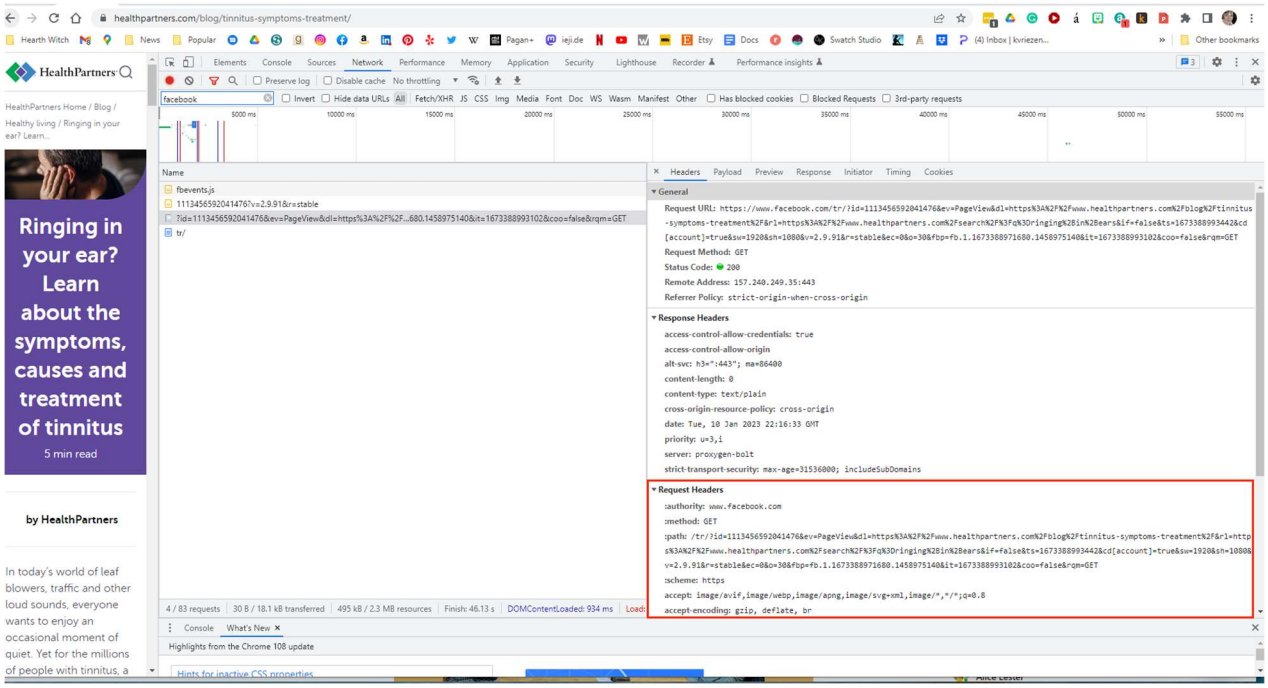
iii. Plaintiff has Specific Evidence of Defendant's Tracking Pixel Communicating with Facebook regarding her Private Information.

118. Plaintiff submitted medical information to Defendant via the Website. Because Defendant utilizes the Facebook Pixel, the Website's Source Code sends a secret

set of instructions back to the individual's browser, causing the Pixel to send Plaintiff's FID, the Pixel ID, and the webpage's URL to Facebook. For instance, when Plaintiff visited Defendant's webpage for e medical condition, the Facebook Pixel reports back the Plaintiff's FID as well as the web page and other data specified by Defendants secretly to Facebook.

119. For example, on January 10, 2023, Plaintiff visited Defendant's Webpage on Tinnitus. Upon Plaintiff visiting the Webpage, the Facebook Pixel (i.e., Pixel ID 111345692041476) sends data, including Plaintiff's communications to/from Defendant, to Facebook.

120. The Pixel sends Plaintiff's data and information from Defendant's Website to Facebook. The screenshot below identifies the following: (1) the Pixel by specific code—111345692041476; (2) Plaintiff's c_user profile, i.e., the FID which identifies her in Facebook by name; and (3) the Facebook Request Header. The Facebook Request Header establishes the Facebook Pixel's transmission of information from Defendant's Website to Facebook.



REQUEST HEADERS (Translated for Human Reading)

:authority: www.facebook.com

:method: GET

:path: /tr/?id=1113456592041476&ev=PageView&dl=https://www.healthpartners.com/blog/tinnitus-symptoms-treatment/&rl=https://www.healthpartners.com/search/?q=ringing+in+ears&if=false&ts=1673388993442&cd[account]=true&sw=1920&sh=1080&v=2.9.91&r=stable&ec=0&o=30&fbp=fb.1.1673388971680.1458975140&it=1673388993102&coo=false&rqm=GET

:scheme: https

accept: image/avif,image/webp,image/apng,image/svg xml,image/*,*/*;q=0.8

accept-encoding: gzip, deflate, br

accept-language: en-US,en;q=0.9

cookie: sb=3weRY-bqFa3SlHGzGX6acUwo; datr=3weRY-OehELhjZhm7U53nofC; c_user=[redacted]; dpr=0.8999999761581421; usida=eyJ2ZXIiOjEsImlkIjoiQXJvMW5vNzFhZXphMWEiLCJ0aWlljoxNjcyOTc0ODcxfQ==; xs=47:PdoYdwg1xPP5vA:2:1670449958:-1:2979::AcXDgqUokr_RFVRhtM-l1q1qc0dGPzq2IsDXVpZLSzI; fr=0fzhD7LYmOm2pvNPu.AWVU_4IB6MAHVn38ouWrA2F5Szo.BjvdWp.Q3.AAA.0.0.BjveHw.AWW40daqjAI

dnt: 1

referer: https://www.healthpartners.com/

sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108", "Google Chrome";v="108"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

sec-fetch-dest: image

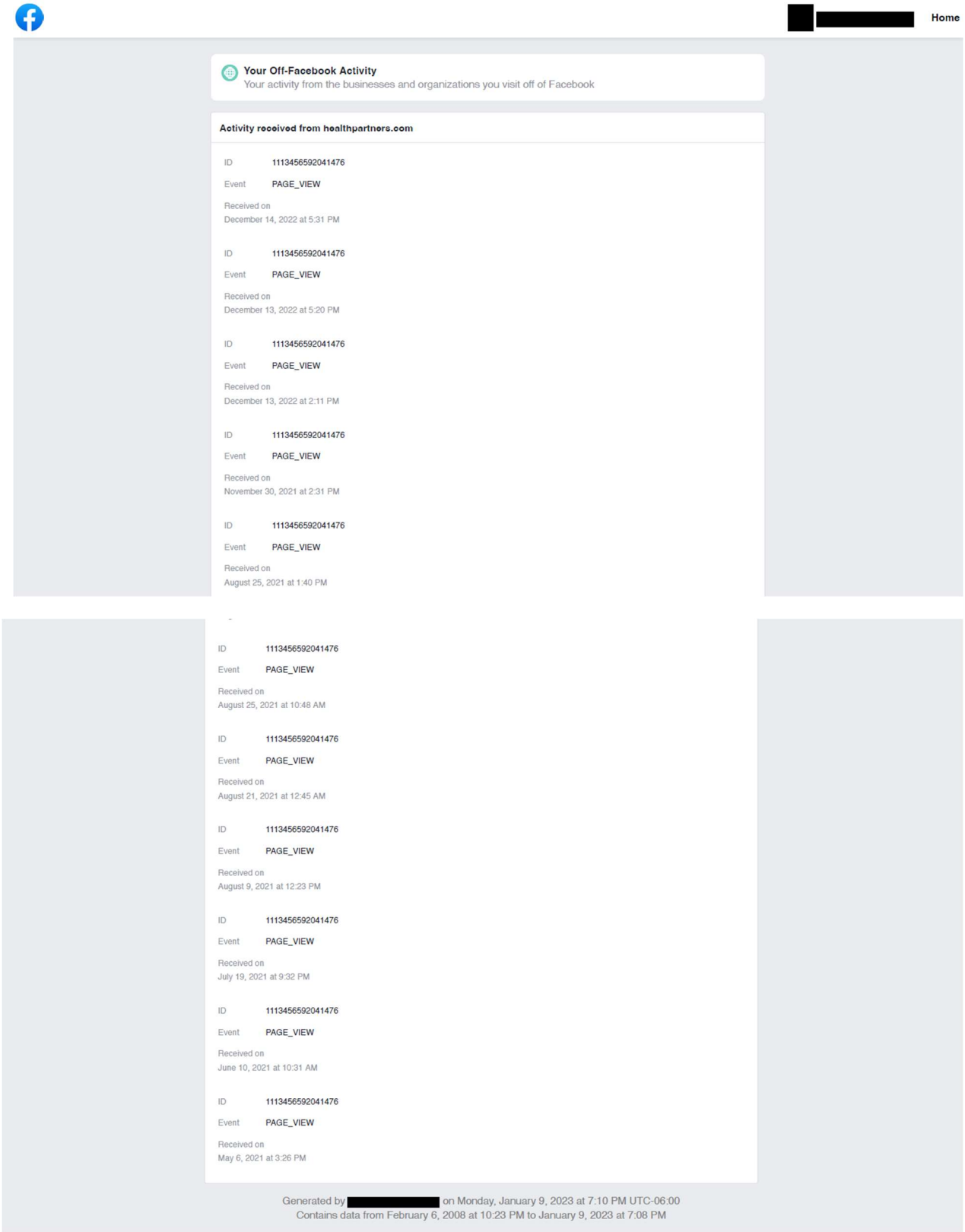
sec-fetch-mode: no-cors

sec-fetch-site: cross-site

user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

121. Additionally, Plaintiff's records show the Defendant's Pixel sent her private

communications with Defendant to Facebook on multiple occasions:



122. Indeed, as the screenshot above demonstrates, Plaintiff's communications with Defendant, and any PII or PHI contained therein, were transmitted to Facebook via Defendant's Pixel.

123. Upon downloading her offsite activity from www.Facebook.com, Plaintiff learned that Defendant's Pixel transmitted her private communications on the following dates: May 6, 2021; June 10, 2021; July 19, 2021; August 9, 2021; August 2, 2021; August 25, 2021 (2x); November 30, 2021; December 13, 2022 (2x); and December 14, 2022.

124. On these dates and times, Plaintiff remembers seeking medical treatment and/or browsing Defendant's website for medical treatment or care. For example, on May 6, 2021 and June 10, 2021, Plaintiff sought and has records of the medical services and treatment she received from Defendant.

125. Accordingly, during the same transmissions, the Website routinely provide Facebook with its patients' FIDs, IP addresses, and/or device IDs or other the information they input into Defendant's Website, like their home address, zip code, or phone number. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.[24] Plaintiff's and Class Members identities could be easily determined based on the FID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

126. After intercepting and collecting this information, Facebook processes it,

[24] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Nov. 14, 2022)

analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the Website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity. A user's Facebook Profile ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

127. In sum, Defendant's Pixel transmitted Plaintiff's highly sensitive communications and Private Information to Facebook, including communications that contained Private and confidential information, without Plaintiff's knowledge, consent, or express written authorization

128. Defendant breached Plaintiff's right to privacy and unlawfully disclosed her Private Information to Facebook. Specifically, Plaintiff had a reasonable expectation of privacy, based on Defendant's Privacy Policy and her status as Defendant's patient, that Defendant would not disclose her Private Information to third parties.

129. Defendant did not inform Plaintiff that it shared her Private Information with Facebook. Moreover, Defendant's privacy policy does not state that its patients' Private Information will be shared with Facebook.

130. By doing so without Plaintiff's consent, Defendant breached Plaintiff's and Class Members' right to privacy and unlawfully disclosed Plaintiff's Private Information.

131. Upon information and belief, as a "redundant" measure to ensure Plaintiff's Class Members' Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's and Class Members' Private Information from electronic storage on Defendant's server directly to Facebook.

132. Plaintiff suffered damages in the form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the invasion of privacy; (iii) diminution of value of the Private Information; (iv) statutory damages; (v) the continued and ongoing risk to her Private Information; and (vi) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiff's medical conditions and other confidential information she communicated to Defendant via the Website.

133. Plaintiff has a continuing interesting in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

C. Defendant's Conduct is Unlawful and Violates its Patients' Rights.

i. Defendant' Conduct Violates its Own Privacy Policies and Promises

134. Defendant's privacy policies represent to Plaintiff and Class Members that Defendant will keep Private Information private and confidential and they will only

disclose Private Information under certain circumstances. [25]

135. Defendant publishes several privacy policies that represent to patients and Website visitors that Defendant will keep sensitive information confidential and will only disclose PII and PHI under certain circumstances, none of which apply here.

136. Defendant's Notice of Privacy Practices explains Defendant's legal duties with respect to Private Information and the exceptions for when Defendant can lawfully use and disclose Plaintiff's and Class Members' Private Information in the following ways:

- Follow the law;
- Help with public health and safety issues;
- Respond to organ and tissue donation requests;
- Work with a medical examiner or funeral director
- Handle workers' compensation;
- Respond to lawsuits and legal actions; and
- With your written permission

137. Defendant's Privacy Policy does not permit Defendant to intercept, transmit, and/or disclose Plaintiff's and Class Members' Private Information to third parties, including Facebook, for marketing purposes.

138. Defendant's Privacy Policy acknowledges Defendant is required by law to maintain the confidentiality of Plaintiff's and Class Members' Private Information, subject

[25]https://www.healthpartners.com/ucm/groups/public/@hp/@public/documents/documents/cntrb_009405.pdf (last visited: January 10, 2023).

to the exceptions listed above.[26]

139. Defendant violated its own Privacy Policy by unlawfully intercepting and disclosing Plaintiff's and Class Members' Private Information to Facebook and third parties without adequately disclosing that it shares Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

ii. Defendant Violated HIPAA Standards

140. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[27]

141. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

142. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at

[26] *Id*.

[27] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

a certain clinic, then this information would be PHI.[28]

143. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added).[29]

144. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[30]

145. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

146. In other words, HHS has expressly stated that Defendant has violated HIPAA

---

28 https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022)

29 https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Nov. 3, 2022)

30 *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

Rules by implementing the Facebook Pixel.

iii. Defendant Violated Industry Standards

147. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

148. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

149. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)

150. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

151. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must…:(c) release patient information only in keeping ethics guidelines for confidentiality.

iv. Plaintiff's and Class Members' Expectation of Privacy

152. Plaintiff and Class Members were aware of Defendant's duty of

confidentiality when they sought medical services from Defendant.

153. Indeed, at all times when Plaintiff and Class Members provided their PII and PHI to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

v. IP Addresses are Personally Identifiable Information

154. On information and belief, through the use of the Facebook Pixel on the Defendant's Website, Defendant also disclosed and otherwise assisted Facebook with intercepting Plaintiff's and Class Members' Computer IP addresses.

155. An IP address is a number that identifies the address of a device connected to the Internet.

156. IP addresses are used to identify and route communications on the Internet.

157. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

158. Facebook tracks every IP address ever associated with a Facebook user.

159. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

160. Under HIPAA, an IP address is considered personally identifiable information:

- HIPAA defines personally identifiable information to include "any unique

identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

161. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

vi. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

162. The sole purpose of the use of the Facebook Pixel on Defendant's Website was marketing and profits.

163. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on its platform.

164. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients.

165. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

TOLLING

166. Any applicable statute of limitations has been tolled by the "delayed

discovery" rule. Plaintiff did not know (and had no way of knowing) that her PII and PHI was intercepted and unlawfully disclosed to Facebook because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

167. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

168. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent as a result of using Defendant's Website (the National Class)**

169. In addition to the claims asserted on behalf of the National Class, Plaintiff asserts claims on behalf of a separate sub-class, defined as follows:

> **All individuals residing in Minnesota whose Private Information was disclosed to a third party without authorization or consent as a result of using Defendant's website (the Minnesota Subclass)**

170. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

171. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

172. Numerosity, Fed R. Civ. P. 23(a)(1). The National Class and Minnesota

Subclass members are so numerous that joinder of all members is impracticable. Upon information and belief, there are over one million individuals whose PII and PHI may have been improperly disclosed to Facebook, and the Class is identifiable within Defendant's records.

173. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant violated its privacy policy by disclosing the PII and PHI of Plaintiff and Class Members to Facebook and/or additional third parties.

d. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient PII and PHI;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

h. Whether Defendant violated the consumer protection statutes asserted as claims in this Complaint;

i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;

k. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices; and

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their PII and PHI.

174. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

175. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

176. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

177. Policies Generally Applicable to the Class. Fed. R. Civ. P. 23(b)(2). This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

178. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and

appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

179. The litigation of the claims is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

180. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

181. Unless a classwide injunction is issued, Defendant may continue disclosing the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

182. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief

with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

183. Issue Certification, Fed. R. Civ. P. 23(c)(4)._Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to, the following:

a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;

b. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information with respect to Defendant's privacy policy;

c. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

g. Whether Class Members are entitled to actual, consequential, and/or nominal

damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

184. Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

COUNT I
INVASION OF PRIVACY
(On Behalf of Plaintiff and the National Class)

185. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

186. The Private Information of Plaintiff and Class Members consist of private and confidential facts and information that were never intended to be shared beyond private communications.

187. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

188. Defendant owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

189. Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information to Facebook, a third-party social media and marketing giant, is highly offensive to a reasonable person.

190. Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Private Information constitutes an intentional interference with Plaintiff's and

the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

191. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiff's and Class Members' privacy because Defendant facilitated Facebook's simultaneous eavesdropping and wiretapping of confidential communications.

192. Defendant failed to protect Plaintiff's and Class Members' Private Information and acted knowingly when it installed the Pixel onto its Website because the purpose of the Pixel is to track and disseminate individual's communications with the Website for the purpose of marketing and advertising.

193. Because Defendant intentionally and willfully incorporated the Facebook Pixel into its Website and encouraged patients to use that Website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff and Class Members.

194. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiff and the Class Members was disclosed to a third party without authorization, causing Plaintiff and the Class to suffer damages.

195. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, plus prejudgment interest, and costs.

196. Defendant's wrongful conduct will continue to cause great and irreparable

injury to Plaintiff and the Class since their PII and PHI are still maintained by Defendant and still in the possession of Facebook and the wrongful disclosure of the information cannot be undone.

197. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook who on information and belief continues to possess and utilize that information.

198. Plaintiff, on behalf of herself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII and PHI and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT II
UNJUST ENRICHMENT
(On behalf of Plaintiff and the National Class)

199. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

200. Defendant benefits from the use of Plaintiff's and Class Members' Private Information and unjustly retained those benefits at their expense.

201. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation. Defendant consciously collected and used this

information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

202. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

203. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in Minnesota and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

204. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT III
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(1) *et seq*.
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of Plaintiff and the National Class)

205. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

206. The ECPA protects both sending and receipt of communications.

207. 18 U.S.C. § 2520(a) provides a private right of action to any person whose

wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

208. The transmissions of Plaintiff's PII and PHI to Defendant via Defendant' Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

209. The transmissions of Plaintiff's PII and PHI to the Virtuwell Webpage and medical professionals qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(2).

210. **Electronic Communications**. The transmission of PII and PHI between Plaintiff and Class Members and Defendant via its Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

211. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

212. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

213. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendant's web-servers; and

d. The Pixel deployed by Defendant to effectuate the sending and acquisition of patient communications

214. By utilizing and embedding the Pixel on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

215. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Private Information to Facebook.

216. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiff's and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

217. By intentionally disclosing or endeavoring to disclose the electronic communications of the Plaintiff and Class Members to affiliates and other third parties,

while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

218. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

219. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

220. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel and Conversions API to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

221. Defendant was not acting under color of law to intercept Plaintiff and the Class Member's wire or electronic communication.

222. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the Pixel tracking code.

223. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

224. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious and designed to violate federal and state legal provisions, including as described above the following: (1) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (2) violation of Minn. Stat. § 325D.44, subd. 1.

COUNT IV
VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE
18 U.S.C. § 2511(3)(a)
(On Behalf of Plaintiff and the National Class)

225. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

226. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

227. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

228. Defendant's Website is an electronic communication service that gives users

the ability to send or receive electronic communications to Defendant and, upon information and belief, medical professionals who contract with, but are not employed by Defendant. In the absence of Defendant's Website, internet users could not send or receive communications regarding Plaintiff's and Class Members' PII and PHI.

229. Defendant's Website is a conduit of communication between Plaintiff and Class Members and their respective medical providers, including third parties who are not employed by Defendant, but contract with Defendant to provide medical treatment and services for its patients.

230. Defendant's Website is also a conduit between Plaintiff and Class Members and the Virtuwell Webpage.

231. **Intentional Divulgence**. Defendant intentionally designed and/or implemented the Pixel and Conversions API tracking and was or should have been aware that it could divulge Plaintiff's and Class Members' PII and PHI.

232. **While in Transmission**. Upon information and belief, Defendant's divulgence of the contents of Plaintiff's and Class Members' communications was contemporaneous with their exchange with Defendant's Website, to which they directed their communications.

233. Defendant divulged the contents of Plaintiff's and Class Members' electronic communications without authorization. Defendant divulged the contents of Plaintiff's and Class Members' communications to Facebook without Plaintiff's and Class Members' consent and/or authorization.

234. **Exceptions do not apply**. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication":

- "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"
- "with the lawful consent of the originator or any addressee or intended recipient of such communication;"
- "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or
- "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

U.S.C. § 2511(3)(b).

235. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

236. Defendant's divulgence of the contents of Plaintiff's and Class Members'

communications on Defendant's Website to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant's service; nor (2) necessary to the protection of the rights or property of Defendant.

237. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

238. Defendant's divulgence of the contents of user communications on Defendant's browser through the Pixel and Conversions API code was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Websites or apps with which Plaintiff and Class Members were exchanging information.

239. Moreover, Defendant divulged the contents of Plaintiff and Class Members' communications through the Facebook Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

240. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

241. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; and reasonable attorneys' fees and other litigation costs reasonably

incurred.

COUNT V
VIOLATION OF
TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2702, *et seq*.
(STORED COMMUNICATIONS ACT)
(On Behalf of Plaintiff and the National Class)

242. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

243. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

244. **Electronic Communication Service.** ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

245. Defendant's Website is a conduit of communication between Plaintiff and Class Members and their respective medical providers, including third parties who are not employed by Defendant, but contract with Defendant to provide medical treatment and services for its patients.

246. Defendant's Website is also a conduit between Plaintiff and Class Members and the Virtuwell Webpage.

247. Defendant intentionally procures and embeds various Plaintiff's PII and PHI through the Pixel and Conversions API used on Defendant's Website, which qualifies as

an Electronic Communication Service.

248. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

249. Defendant stores the content of Plaintiff's and Class Members' communications with Defendant's Website and files associated with it via the Pixel or Conversions API. As explained above, via Conversions API, Defendant stores Plaintiff's and Class Members' Private Information on its servers and then transmit that Private Information to Facebook.

250. By way of another example, Defendant stores data pertaining to scheduling appointments, IP addresses, and communications regarding medical treatment.

251. When Plaintiff or Class Member communicates with the Website, the content of that communication is immediately placed into storage.

252. Defendant knowingly divulges the contents of Plaintiff's and Class Members' communications through its Website' source code.

253. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—"

a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."

b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;"

c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"

d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"

e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;"

f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A."

g. "to law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;"

h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or

i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

254. Defendant did not divulge the contents of Plaintiff's and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiff and Class Members.

255. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

256. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

257. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on Defendant's Website to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of the Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

258. Defendant's divulgence of the contents of user communications on Defendant's Website was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Websites or apps with which Plaintiff and Class Members were exchanging information.

259. Moreover, Defendant divulged the contents of Plaintiff's and Class Members' communications through the Facebook Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

260. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

261. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages if applicable in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT VI
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (CFAA) 18 U.S.C. § 1030, ET SEQ.
(On Behalf of Plaintiff and the National Class)

262. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

263. The Plaintiff's and the Class Members' computers and/or mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

264. Defendant exceeded, and continues to exceed, authorized access to the Plaintiff's and the Class Members' protected computers and obtained information thereby, in violation of 18 U.S.C. §§ 1030(a)(2), 1030(a)(2)(C).

265. For example, Defendant exceeded its unauthorized access because Defendant accessed Plaintiff's and Class Members' Private Information under false pretenses, *i.e.*, Defendant did not disclose it was transmitting Private Information to Facebook.

266. Moreover, Defendant exceeded its unauthorized access because Defendant

violated its *own* Privacy Policies in disclosing Plaintiff's and Class Members' Private Information to Facebook.

267. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiff's and the Class Members' private and personally identifiable data and content – including the Website visitor's electronic communications with the Website, URLs of web pages visited, and/or other electronic communications in real-time which were never intended for public consumption.

268. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV) due to the Private Information of Plaintiff and the Class being made available to Defendant, Facebook, and/or other third parties without adequate legal privacy protections.

269. Accordingly, Plaintiff and the Class are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

COUNT VII
BREACH OF CONFIDENCE
(On behalf of Plaintiff and the National Class)

352. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

353. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

354. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website, which were further buttressed by Defendant's express promises in its privacy policy.

355. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Pixel and Conversions API to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant, including Private Information and the contents of such information.

356. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

357. The third-party recipients included, but may not be limited to, Facebook.

358. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

359. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;

b. Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

d. General damages for invasion of their rights in an amount to be determined by a jury;

e. Nominal damages for each independent violation;

f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;

g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and

i. Defendant's actions violated the property rights Plaintiff and Class members have in their Private Information.

COUNT VIII
Minnesota Uniform Deceptive Trade Practices Act ("MUDPTA") Minn. Stat. §325D.43-48
(On behalf of Plaintiff and the Minnesota Class)

360. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

361. The MDUPTA prohibits deceptive trade practices in person's business, vocation, or occupation. *See* Minn. Stat. § 325D.44, subd. 1.

362. Defendant advertised, offered, or sold goods or services in Minnesota and therefore engaged in business directly or indirectly affecting the people of Minnesota, Defendant violated Minn. Stat. § 325D.44, including, but not limited to, the following provisions:

a. represents that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and

b. Engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.

363. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the MDUPTA, including, but not limited to, the following: (1) promising to protect Plaintiffs' and Class Members' Private Information via its Privacy Policies and then, in fact, knowingly, transmitting Plaintiffs' and Class Members' Private Information to third parties, such as Facebook; (2) unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook; (3) failing to disclose or omitting material facts that that Plaintiffs' and Class Members' Private Information would be disclosed to third parties; (4) failing to obtain Plaintiffs' and Class Members' consent in transmitting Plaintiffs' and Class Members' Private Information to Facebook; and (5) knowingly violating industry and legal standards regarding the protection of Plaintiffs' and Class Members' Private Information.

364. These actions also constitute deceptive and unfair acts or practices because Defendant knew its Website contained the Pixel and Conversions API and also knew the Pixel and Conversions API would be unknown and/or not easily discoverable by Plaintiffs and Class Members.

365. Defendant intended that Plaintiff and the Minnesota Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

366. Had Defendant disclosed to Plaintiff and the Minnesota Class that its Website was transmitting PII and PHI to Facebook via the Pixel and Conversions API, Plaintiff and the Minnesota Class would not have provided their Private Information to Defendant.

367. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Minnesota Class. Plaintiff and the Minnesota Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

368. As a result of Defendant's wrongful conduct, Plaintiff and the Minnesota Class were injured in that they never would have provided their PII and PHI to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII and PHI from being taken and misused by others.

369. As a direct and proximate result of Defendant's violations of the MDUPTA, Plaintiff and the Minnesota Class have suffered harm, including actual instances of identity

theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiff and the Minnesota Class would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII and PHI; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

370. Pursuant to MDUPTA, Plaintiff and the Minnesota Class are entitled to injunctive relief and other appropriate relief, as alleged.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the National Class and Minnesota Subclass and appointing Plaintiff and Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members:

D. For an award of damages, including, but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand that this matter be tried before a jury.

DATE: February 2, 2023

Respectfully Submitted,

/s/ Bryan L. Bleichner
Bryan L. Bleichner (MN BAR #0326689)
Jeffrey D. Bores (MN BAR #0227699)
Philip J. Krzeski (MN BAR #0403291)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
jbores@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Gary M. Klinger*
Alexandra M. Honeycutt*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court St., Ste. 530
Cincinnati, Ohio 4502
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Joseph M. Lyon*
The Lyon Law Firm
2754 Erie Ave.
Cincinnati, Ohio 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Counsel for Plaintiff and the Putative Class

* *pro hac vice* forthcoming